ГО «ГРУЗИНСЬКО-УКРАЇНСЬКИЙ ЕКСПЕРТНИЙ ЦЕНТР»

# СУЧАСНІ ЗАГРОЗИ ГЛОБАЛЬНІЙ ТА РЕГІОНАЛЬНІЙ БЕЗПЕЦІ

МАТЕРІАЛИ
Міжнародної науково-практичної інтернет-конференції
*(м. Одеса, 29 жовтня 2023 року)*

DOI: 10.46340/GUEC2023-10

Одеса
Фенікс
2023

УДК 327.7:355.02
С 89



**Сучасні загрози глобальній та регіональній безпеці** : матер. С 89 Міжнар. наук.-практ. інтерн.-конф. (м. Одеса, 29 жовтня 2023 р.) [Електронне видання] / уклад. А. Полухіна ; ГО «ГУЕЦ». – Одеса : Фенікс, 2023. – 389 с. –Укр., англ., груз. мовами.

ISBN 978-617-8395-01-8

Збірник матеріалів містить матеріали доповідей, поданих на Міжнародну науково-практичну інтернет-конференцію «Сучасні загрози глобальній та регіональній безпеці», що відбулася 29 жовтня 2023 року. Подані матеріали були розглянуті під час роботи дев'яти секцій: теоретичні та прикладні аспекти міжнародного співробітництва у сфері безпеки; криза сучасної системи міжнародної безпеки; регіональна безпека в нових геополітичних концепціях; основні стратегічні напрямки кібербезпеки; кіберзахист і національна безпека: український досвід; цифрова дипломатія в умовах трансформації системи міжнародної безпеки; фейки та діпфейки як інструменти негативного впливу на національну безпеку; фактчекінг як інструмент протидії в гібридній війні; державне управління та національна безпека.

Збірник адресовано науковим, науково-педагогічним працівникам, здобувачам закладів вищої освіти, громадським організаціям, журналістам, незалежним експертам і всім, хто цікавиться проблемами загроз глобальній та регіональній безпеці.

**УДК 327.7:355.02**



ISBN 978-617-8395-01-8

# З М І С Т

## ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ АСПЕКТИ МІЖНАРОДНОГО СПІВРОБІТНИЦТВА У СФЕРІ БЕЗПЕКИ

## КРИЗА СУЧАСНОЇ СИСТЕМИ МІЖНАРОДНОЇ БЕЗПЕКИ



## РЕГІОНАЛЬНА БЕЗПЕКА В НОВИХ ГЕОПОЛІТИЧНИХ КОНЦЕПЦІЯХ

## ОСНОВНІ СТРАТЕГІЧНІ НАПРЯМКИ КІБЕРБЕЗПЕКИ

## КІБЕРЗАХИСТ ТА НАЦІОНАЛЬНА БЕЗПЕКА: УКРАЇНСЬКИЙ ДОСВІД



## ЦИФРОВА ДИПЛОМАТІЯ В УМОВАХ ТРАНСФОРМАЦІЇ СИСТЕМИ МІЖНАРОДНОЇ БЕЗПЕКИ

## ФЕЙКИ ТА ДІПФЕЙКИ ЯК ІНСТРУМЕНТИ НЕГАТИВНОГО ВПЛИВУ НА НАЦІОНАЛЬНУ БЕЗПЕКУ



## ФАКТЧЕКІНГ ЯК ІНСТРУМЕНТ ПРОТИДІЇ В ГІБРИДНІЙ ВІЙНІ



## ПУБЛІЧНЕ УПРАВЛІННЯ ТА НАЦІОНАЛЬНА БЕЗПЕКА

## ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНІ ДЕТЕРМІНАНТИ ФОРМУВАННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

**Куля Ірина Федорівна**
*Придунайська філія МАУП, м. Ізмаїл, Україна*
**ORCID:** 0000-0002-8363-1478

**Беженар Карина Дмитрівна**
*Придунайська філія МАУП, м. Ізмаїл, Україна*

# ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА

В сучасному світі все частіше постає проблема збільшення інформаційної безпеки підприємств, яка залежить саме від ступеня захищеності інформаційної сфери. Збереження стабільності функціонування та економічного росту, розвиток науково-технічних інновацій залежать від правильної організації інформаційної захищеності підприємств.

Глобальний розвиток інформаційних технологій, модернізована обробка інформації спостерігаються зі зростанням науково-технічного прогресу. Разом з цим і підвищується роль інформаційної безпеки підприємств.

При веденні діяльності кожен підприємець в обов'язковому порядку зіштовхується з необхідністю отримання, зберігання, обробки, перетворення, поширення, передачі та видалення непотрібної або зайвої інформації. Інформація, яка несе користь для підприємства має бути захищеною від зловмисників. При захисті інформації слід перекрити всі канали можливого витоку та забезпечити безпеку зберігання інформації на усіх носіях, що маються на підприємстві.

Згідно законодавства України інформаційна безпека – це стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації (Про основні засади розвитку інформаційного суспільства).

Потреба в володінні інформацією призводить до оволодіння інформацією про навколишнє середовище та процеси, що протікають в ньому, тобто інформованості індивіда, соціуму та держави.

Стан та ступінь інформованості впливає на майбутні дії, а також на обґрунтування рішень, які прийматимуться підприємцями.

Загрози інформаційній безпеці – це сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам підприємств чи підприємців в інформаційній сфері.

Фактори загроз інформаційній безпеці можна класифікувати за видами та ієрархією (рис.1).


***Рис. 1. Класифікація факторів загроз інформаційній безпеці***

В залежності від виду загроз, інформаційну безпеку можна розглядати як забезпечення стану захищеності (Герасименко, Козак, 2015):

– особистості, суспільства та держави від впливу недостовірної інформації;

– підприємств, організації та інших установ;

– інформації та інформаційних ресурсів від неправомірного впливу сторонніх осіб;

– інформаційних прав і свобод громадянина.

Належний рівень інформаційної безпеки забезпечується сукупністю економічних, організаційних, політичних заходів, спрямованих на попередження, виявлення і нейтралізацію таких обставин, дій і факторів, які можуть завдати шкоди і збитків або перешкодити реалізації інформаційних прав, потреб та інтересів підприємств (Про основні засади розвитку інформаційного суспільства).

Основним і головним завданням заходів з інформаційної безпеки є мінімізація шкоди за неповноти, несвоєчасності або недостовірності інформації чи негативного інформаційного впливу через наслідки функціонування інформаційних технологій, а також несанкціоноване поширення інформації.

Забезпечення інформаційної безпеки має бути спрямоване саме на запобігання ризиків, а не на ліквідацію їх наслідків. Тому прийняття запобіжних заходів для забезпечення цілісності, конфіденційності, а також доступності інформації і є найбільш правильним підходом у створенні системи інформаційної безпеки. Будь-який витік інформації може призвести до серйозних проблем для підприємства – від значних фінансових збитків до повного припинення існування підприємства (Северина, 2016).

Одним з головних елементів системи інформаційної безпеки підприємств виступають принципи, які мають закладатися в основу її побудови. Основними принципами інформаційної безпеки підприємств є: простота, повний контроль, загальна заборона, відкрита архітектура, розмежування доступу, мінімальні привілеї, стійкість, мінімізація дублювання (рис. 2).

Принцип простоти наголошує на тому, що простота в використанні інформаційної системи здатна забезпечити мінімізацію помилок.

Повний контроль полягає в передбаченні підприємством безперервного контролю за станом інформаційної безпеки та моніторингу всіх подій, що впливають на інформаційну безпеку.

Загальна заборона полягає в забороні доступу до інформаційної системи підприємства, без наданого на це дозволу.

Принцип відкритої архітектури полягає в тому, що безпека має забезпечуватися через неясність. Спроби захистити інформаційну систему від комп'ютерних загроз шляхом заплутування, ускладнення, приховування слабких міст і сторін.

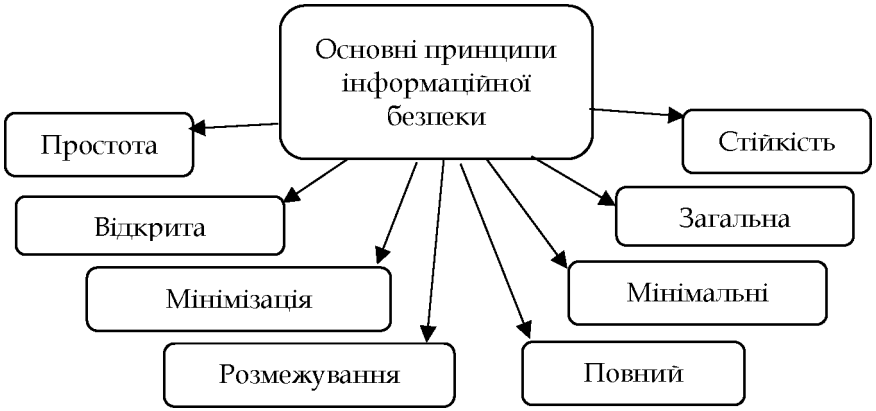


***Рис. 2. Основні принципи інформаційної безпеки***

Принцип розмежування доступу полягає в тому, що кожному користувачеві надається доступ до інформації, а також її носіїв у відповідності до його повноважень.

Принцип мінімальних привілеїв полягає у виділенні користувачам найменших прав і мінімального доступу до інформаційної системи.

Принцип стійкості інформаційної системи виражається в тому, що потенційні зловмисники мають зустрітися з перешкодами, складними обчислювальними завданнями при потенційній хакерській атаці.

Мінімізація дублювання передбачає мінімізацію ідентичних процедур для декількох споживачів, наприклад, таких як введення паролів.

Побудована за наведеними принципами система інформаційної безпеки має бути налаштована на досягнення визначених цілей, специфіка яких буде великою мірою визначати структуру системи і основні параметри її функціонування (Рудий, Томаневич, Руда, 2014).

Для підприємств основними цілями досягнення високого рівня інформаційної безпеки є забезпечення її основних складових: цілісності, достовірності, конфіденційності (рис. 3).

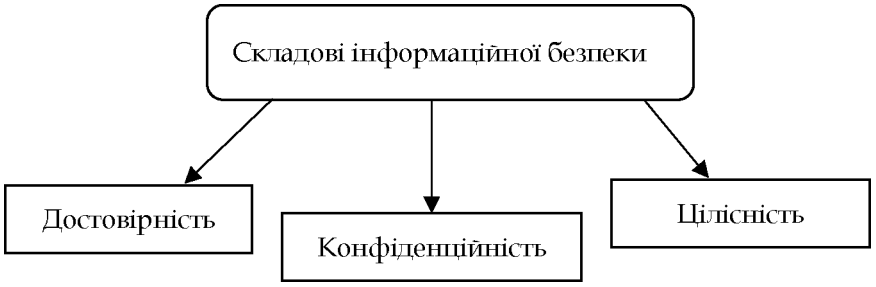


***Рис. 3 Складові інформаційної безпеки***

Доступність – це можливість за певний період часу одержати необхідну інформаційну послугу.

Цілісність – це актуальність і несуперечність інформації, її захищеність від змін та видалення. В свою чергу цілісність можна розділити на статичну (розуміється як незмінність інформаційних об'єктів) і динамічну (відноситься до коректного виконання певних дій та складних транзакцій).

Конфіденційність – властивість інформації, яка полягає в тому, що інформація не може бути отримана і поширена серед певного кола індивідів.

Успішність функціонування підприємств у динамічному ринковому середовищі значною мірою визначається станом інформаційної безпеки. Рівень економічної безпеки суб'єкта господарювання залежить від того, наскільки ефективною є інформаційна безпека суб'єкта господарювання, що дає змогу уникнути можливих загроз та негативних наслідків впливу конкурентного середовища.

Отже, безпека підприємства – це такий стан корпоративних ресурсів (ресурсів капіталу, персоналу, інформації і технології, техніки та устаткування, прав) і підприємницьких можливостей, за якого гарантується найбільш ефективне їхнє використання для стабільного функціонування та динамічного науково-технічного й соціального розвитку, запобігання внутрішнім та зовнішнім негативним впливам (загрозам) (Архипов, Скиба, 2013).

Відповідно достатній рівень інформаційної безпеки дає змогу підприємству повною мірою використовувати необхідну інформацію для прийняття результативних управлінських рішень, виконання яких обумовить подальшу фінансову стійкість підприємства і буде сприяти його подальшій ефективній роботі (Войнаренко, Рзаєв, Рзаєва, 2014).

### *Література*

Архипов, О., Скиба, А. (2013). Інформаційні ризики: методи та способи дослідження, моделі ризиків і методи їх ідентифікації. *Захист інформації, 15, 4,* 350–375.

Василенко, М. (2018). Підвищення стану кібербезпеки інформаційно комунікаційних систем: якість у контексті вдосконалення інформаційного законодавства. *Юридичний вісник, 3,* 17–24.

Герасименко, О. В., Козак, А. В. (2015). *Інформаційна безпека підприємства: поняття та методи її забезпечення*. URL: http://intkonf.org/ken-gerasimenko-ov-kozak-av-informatsiyna-bezpeka-pidpriemstva-ponyattya-ta-metodi-yiyi-zabezpechennya/

Іванова, В. *Інформаційна безпека як підсистема в системі економічної безпеки підприємства*. URL: http://eprints.kname.edu.ua/38599/1/67–71.pdf.

Войнаренко, М. П., Рзаєв, Г. І., Рзаєва, Т. Г. (2014). *Інформаційна безпека підприємства у динамічному ринковому середовищ*. Хмельницький.

*Закон про сновні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки Закон України 2007* (Верховна Рада України). *Офіційний сайт Верховної Ради України.* URL: https://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=537-16#Text

Рудий, Т., Томаневич, Л., Руда, О. (2014). Засади захисту інформації в інформаційних системах підприємств. *Актуальні проблеми економіки, 2 (152),* 351–387.

Северина, С. (2016). Інформаційна безпека та методи захисту інформації. *Вісник Запорізького національного університету. Економічні науки, 1,* 132–154.